Information Commissioner's Office
Wycliffe House
Water Lane,
Wilmslow
Cheshire SK9 5AF
via datasharingcode@ico.org.uk.

FAO: Steve Wood, Deputy Information Commissioner

Response of the National Motorists Action Group to the ICO consultation on the draft Code of Data Sharing v.1

We are nearing completion of a detailed report to the Commissioner that shows long-standing serious misconduct of the DVLA in breach of the data protection legislation.

It concerns the massive on-going release of vehicle keeper personal data to private parking companies (PPCs) for the express purpose of the PPCs pursuing motorists for alleged infringements of PPCs' terms and conditions of parking on the private land parking sites that they manage

The basis of the DVLA's fully-evidenced misconduct soon to be presented is, very briefly, as follows:

- The legitimate statutory basis for DVLA release of vehicle keeper data to any requester is the requester having reasonable cause for each such request. The release of vehicle keeper data to any 'approved' PPC, currently by automated bulk requests without involvement of the DVLA, would clearly be unobjectionable and reasonable, but **only** if a PPC is using the received data for conducting its business in accordance with all applicable law – which PPCs are not.
- The DVLA's automated bulk release of vehicle keeper data automatically on PPC request is expressly dependent on a standardised contractual agreement between the DVLA and each PPC – a 'KADOE Service Contract' (KSC). Release of vehicle keeper data to any particular PPC is therefore lawful **provided** that the PPC is in compliance with the DVLA's terms and conditions prescribed in each KSC. KSC terms and conditions expressly require that the PPC contractor must comply with all requirements of the law in their parking management operations.
- The ongoing unlawful release of personal data by the DVLA arises because PPCs (seemingly all of them, in the order of 200) are, and have long been, in criminal breach of statutory conditions that apply to every private land parking site.
- The forthcoming report to the Commissioner shows that, not only is the DVLA releasing these data erroneously despite PPCs' clear breaches of their KSCs, the DVLA are releasing the data by way of their own misconduct for **knowing** of the illegalities of PPC parking management, the consequential PPC non-compliances with their KSCs, and have long been wilfully refusing to cease the consequently-unlawful data release.

Here-following comments on the draft Code

The draft Code is seen to be a masterly document constructed and formatted with the highest quality and with great diligence.

We have no competence to find fault with any of it and do not do so. However, in light of the brazen data-release misconduct of the DVLA summarised above we are concerned that they, or any other organisation or person engaged in the release of personal data, can purport a lawful power to do so in disregard of a situation in which a data recipient uses the personal data unlawfully, or in furtherance of an unlawful activity, inevitably always to the frequently-severe detriment of the data subjects.

It seems to us obvious that any release of personal data in furtherance of an appropriate power to do so must, despite an absence of any conditional provision in the enabling power must *inter alia* impliedly be conditional on the recipient not using the received data in furtherance of any unlawful conduct.

Notwithstanding that the ICO already has no hindrance to investigating and responding to any received complaint of erroneous data-release such as our report soon to be presented, it seems to us that some cautionary conditions that should over-ride a power and lawfulness to release personal data could usefully be added for completeness into this draft Code where appropriate.

These following comments are inelegantly repetitive but we make them where the draft Code seems to be subject to cautionary conditions that could usefully be stated.

If the ICO approves our suggested supplementation of existing Code texts it will be, of course, for the ICO to decide how and where in the Code it will be best achieved.

Yours sincerely, by email

[redacted]

[redacted] (please reply by email)

Our comments on parts of the draft Code here follow:

Comments with reference to page-numbered content of the draft Code

p. 32. **Accountability**

At a glance

The accountability principle means that you are responsible for your compliance with the GDPR or DPA, as appropriate. You must be able to demonstrate that compliance by:

- carrying out data protection impact assessments (DPIAs) for any data sharing
- that is likely to result in high risk to the interests of individuals;

What is the Accountability principal?

There is a general obligation to evidence your compliance and justify your approach, so you should adopt additional measures as necessary. A data sharing agreement would be one example of good practice to demonstrate your accountability. If you are unable to justify your approach, an accountability breach is likely, regardless of the outcome. The importance of the accountability principle cannot be overstated. To be effective, you have to embed the message of accountability in the culture and business of your organisation, from Board level through all your employees.

comment: High risk to the interests of individuals will arise if their shared personal data is used to their detriment by reason of use by the recipient in unlawful or illegal circumstances. All available measures must be taken by a data sharer to ensure that there is no misuse of the data by or on behalf of the recipient.

p. 33. **What is data protection by design and default?**

"Data protection by design and default" is a legal obligation requiring you to put in place appropriate technical and organisational measures to:

- implement the data protection principles in an effective manner; and
- safeguard individual rights.

comment: Safeguarding of individual rights in compliance with the data protection principles will include the taking all available technical and organisational measures to ensure that there is no unlawful misuse of the shared data by the recipient of the data.

p. 37. **Lawful basis for sharing personal data**

At a glance

You must identify at least one lawful basis for sharing data from the start. You must be able to show that you considered this beforehand, in order to satisfy the accountability principle.

What are the provisions on lawful basis?

You must identify at least one lawful basis for sharing data, from a number of provisions which are different for the GDPR and for Law Enforcement Processing under Part 3 of the DPA. This is known as a lawful basis for processing, and at least one must apply from the start of your data sharing. You must be able to show that you considered this before you started data sharing, in order to satisfy the accountability principle in the GDPR and Part 3 of the DPA. And without at least one lawful basis for processing, any data sharing you do will be in breach of the first principle in each piece of legislation.

comment: Having one *prima facie* lawful basis, or more, for sharing data will not enable lawful sharing of the data unless the sharer has diligently taken all available steps to ensure that no unlawful conduct is involved in the recipient's use of the shared data.

p. 37,38 **Lawful basis under the GDPR**

For data sharing under the GDPR (and under Part 2 of the DPA), there are six lawful bases for processing, contained in Article 6. In summary they are as follows.

(a) Consent: the individual has given their clear consent for you to share their personal data for a specific purpose.

(b) Contract: the sharing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

comment: Where data is shared on the basis of, and in the terms of, a contractual agreement with a recipient, that basis of sharing will be lawful only insofar as the recipient contractor fully complies with the terms of the data-sharing contract. It is incumbent on the data sharer to monitor and enforce full compliance of the recipient with the data-sharing contract to ensure the lawfulness of the contractual basis for sharing.

(e) Public task: the sharing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

comment: A data sharer will have a clear basis in law in furtherance of a task or function to share data provided that the recipient is assured not to misuse the received data. The public interest can never accommodate any misuse of personal data regardless of a necessary task or function under which data sharing may be ostensibly permissible.

(f) Legitimate interests: the sharing is necessary for your legitimate interests or those of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests, especially where the individual is a child. You cannot use legitimate interests as your lawful basis if you are a public authority processing data to perform your official tasks.

comment: No misuse of personal data by a recipient of it can constitute a legitimate interest of a recipient. Any actual or probably-intended misuse of received data that is known or readily knowable to a data holder will inherently preclude lawful supply of it by a data holder.

p. 39. **What do we need to do if we are relying on legitimate interests as our lawful basis?**

If you are relying on legitimate interests as your lawful basis for disclosing data to a third party, you must carry out a three-part test known as a legitimate interests assessment (LIA). This test considers some of the same questions as a DPIA, considering the necessity of the data sharing as well as individual rights.

comment: The rights of any individual whose data is subject to being shared preclude any unlawful misuse of the data by a recipient, and the interests of a recipient cannot be legitimate if the recipient misuses or intends to misuse it after receipt.

p.40 **Fairness and transparency in data sharing**

At a glance

You must always share personal data fairly and in a transparent manner.

- You must treat individuals fairly and not use their data in ways that would have unjustified adverse effects on them.

comment: It will be unlawful for unfairness to share personal data when it is known or knowable to a data holder that the recipient will or is likely to misuse the data after its receipt to the detriment or potential detriment of the data subject.

p. 43. **How do we comply with the fairness principle when sharing data?**

This principle applies to general processing under the GDPR and to processing under Part 3 of the DPA.

- You must treat individuals fairly and not use their data in ways that would have unjustified adverse effects on them.
- You must also ensure that the sharing happens in a way that people would not find unexpected or objectionable, unless there is a good reason. This is the case unless you are sharing due to a legal obligation or the sharing is necessary for law enforcement; the data sharing will take place despite any such concerns.
- You must comply with the fairness principle regardless of the type of sharing: whether you are sharing data on a routine basis or making a single one-off disclosure.
- You must meet the fairness requirement in data sharing in addition to demonstrating that you have a lawful basis for it. If any aspect of your processing is unfair, you will be in breach of the fairness principle – even if you can show that you have a lawful basis for the processing.

comment: If a data recipient is misusing personal data or is suspected of possibly doing so the data subjects will be, or are likely to be, unfairly subject to adverse effects in breach of the fairness principle.

Data subjects, in particular if many are similarly affected by misuse of their data by a data recipient, are bound to find the situation objectionable. The enabling by a data sharer of this situation by their inadequate control of the conduct of a data recipient will breach the fairness principle.

p. 53. **What do we need to do if the data sharing involves automated decision-making?**

If your data sharing arrangement involves any automated decision-making, you must document the specific lawful basis for that automated decision-making in your data protection policy.

comment: Having a properly-documented basis for sharing personal data, that is identifiable as being a lawful basis on the expectation and intention of lawful conduct on the part of a data recipient, will cease to be a lawful basis in the event of relevant unlawful conduct on the part of a data recipient. It is incumbent on a data sharer to take all reasonable measures to ensure there is no misuse of shared data by the recipient.

p. 57 **Other legal requirements**

At a glance

In addition to identifying a lawful basis for your data sharing, you must ensure that your data sharing is lawful in a more general sense in order to comply with the lawfulness principle. For public sector bodies this includes identifying whether you have a legal power to share data.

comment: A data sharer will breach the lawfulness principle if the sharing is not lawful in a more general sense where a data recipient is using, or intends to use, the received data in pursuance of any unlawful conduct, and the data sharer has failed to take all reasonably-available steps to discover the mischief in such a situation and discontinue data sharing.

p.93. **GDPR data protection principles**

Article 5 Principles relating to processing of personal data

1. Personal data shall be:

   1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

comment: Personal data will not be processed either lawfully or fairly if it is reasonably knowable to the sharer that the recipient is or is likely to be using the data in pursuance of any unlawful activity.